

Editor's column

Stuart Krohn

In 2012, *The Next Wave (TNW)* devoted two issues to cybersecurity, focusing on the need for basic scientific foundations to underpin our trust in systems. Creating this "Science of Security" (SoS) requires sustained support and long-term vision. One only needs to look at the news headlines to observe that the need for more secure systems continues to exist and our efforts are far from over.

The good news, I believe, is that we are beginning to see the emergence of some components necessary for a true science—including a community of cybersecurity researchers whose methods are rigorous, who are willing to challenge, refute, and improve ideas, and who are providing results that can be built upon by others. In addition, more and more universities are adding undergraduate and graduate courses or units that examine scientific rigor in security research.

Of course, it is essential that this new science be grounded on common definitions. Throughout the years, there has been much debate about the nature of science—what it is, and what methods are best. The works of Karl Popper on falsifiability, of Pierre Duhem on the testing of hypotheses as parts of whole

bodies of theory, and of Thomas Kuhn on shifts in scientific paradigms, are fine examples of this. No doubt we will continue that broader discussion in relation to security science, but that is not our interest here.

It is essential that this new science be grounded on common definitions.

This issue of *TNW* describes research contributing to the development of security science. Included are highlights of two workshops initiated by the Special Cyber Operations Research and Engineering subcommittee: one on the adoption of cybersecurity technology, the other on computational cybersecurity in compromised environments. We also present highlights of the ongoing multidisciplinary university research at the SoS lablets. Interspersed are several more in-depth papers on topics including power grid security, phishing, privacy, cyber-physical systems, and a competition aimed at building better code.







Whether you are a long-time reader of *TNW* or have just discovered it, we hope you will always count on this publication as a "go to" source for news on emerging technologies.





Stuart Krohn Technical Director, Science of Security Strategic Engagements, NSA

[Cover photo credits: pialhovik, princessmaro/iStock/Thinkstock, Wavebreakmedia Ltd/Wavebreak Media/Thinkstock, Marie Reed]

Contents

2 Resilient and secure cyber-physical systems

WILLIAM EMFINGER, PRANAV SRINAVAS KUMAR, GABOR KARSAI

- 8 Improving power grid cybersecurity
- 12 Analyzing the cost of securing control systems

Zhenqi Huang, Yu Wang, Sayan Mitra, Geir Dullerud

18 Build it, break it, fix it: Competing to build secure systems

MICHAEL HICKS, ANDREW RUEF

24 The social engineering behind phishing Christopher B. Mayhorn, Emerson Murphy-Hill, Olga A. Zielinska, Allaire K. Welk

- 32 GLOBE AT A GLANCE: NSA Science of Security research network
- 34 POINTERS: Science of Security research and events highlights
- 41 FROM LAB TO MARKET: NSA shares cyber software via open source

The Next Wave is published to disseminate technical advancements and research activities in telecommunications and information technologies.

Mentions of company names or commercial products do not imply endorsement by the US Government.

This publication is available online at http://www.nsa.gov/research/tnw/tnw211/article1.shtml.
For more information, please contact us at TNW@tycho.ncsc.mil.